

GEKP

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

19 6019

NICHOLAS RAPAK, individually and on
behalf of himself and all other persons similarly
situated,

Plaintiff,

vs.

WAWA, INC.,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff, Nicholas Rapak ("Plaintiff"), by and through his undersigned counsel, brings this Class Action Complaint against Defendant Wawa, Inc. ("Defendant" or "Wawa"), individually and on behalf of all others similarly situated, and alleges as follows, upon personal knowledge as to himself and his own acts and experiences, and as to all other matters, upon information and belief.

INTRODUCTION

1. Plaintiff brings this class action complaint on behalf of a class of persons harmed as a result of Defendant's failure to safeguard and protect its customers' highly sensitive personally identifiable information ("PII") including, but not limited to: credit and debit card numbers, expiration dates, and names on payment cards used on Wawa's in-store payment terminals and fuel dispensers.

2. On December 19, 2019, Wawa issued a press release¹ on its website stating that it experienced a "data security incident" (the "Data Breach"). Wawa stated that it discovered

¹ An Open Letter from Wawa CEO Chris Gheysens to Our Customers, *available at* <https://www.wawa.com/alerts/data-security> (Dec. 19, 2019).

malware (the “Malware”) on its payment processing servers on December 10, 2019. This Malware affected customers “at potentially all Wawa locations” at some point between March 4, 2019 and December 12, 2019 (the “Class Period”). The Malware was present on most store systems by April 22, 2019.

3. The Malware affected payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019.

4. Because Plaintiff’s PII has been compromised as a result of the Data Breach, Plaintiff and Class Members have been placed at an immediate and continuing risk of identity theft-related harm.

5. As a result of Wawa’s conduct, Plaintiff and Class Members will be required to undertake expensive and time-consuming efforts to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

6. Furthermore, Plaintiff and Class Members will be required to purchase credit and identity monitoring services to alert them to potential misappropriation of their identity and to combat risk of further identity theft. At a minimum, Plaintiff and Class Members have suffered compensable damages because they will be forced to incur the cost of a monitoring service which is a reasonable and necessary step to prevent and mitigate future loss.

THE PARTIES

7. Plaintiff Nicholas Rapak is a resident of Montgomery County, Pennsylvania. Plaintiff Rapak made purchases using Wawa's in-store payment terminals and/or fuel dispensers at numerous Wawa locations between March 2019 and December 2019 with his debit and/or credit card. As such, Plaintiff's PII was stored on Wawa's payment processing servers, and he was affected by the undisclosed Malware.

8. Plaintiff Rapak became aware of the Data Breach through news reports on or about December 19, 2019.

9. Plaintiff has taken precautions to protect his PII. Exposure of Plaintiff's PII as a result of the Data Breach has placed him at immediate and continuing risk of further identity theft-related harm.

10. Defendant Wawa, Inc. ("Wawa") is a privately held domestic New Jersey corporation having its principal executive offices located at 260 W. Baltimore Pike, Wawa, Pennsylvania 19063.

11. Wawa owns and operates more than 850 convenience retail stores (over 600 offering gasoline), in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Wawa services over 800 million customers annually according to 2018 data from the National Association of Convenience Stores.²

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 Class Members, and at least

² NACS, https://www.convenience.org/Media/Daily/ND0523183_Behind-the-Scenes-at-Wawa_Operations (May 23, 2018).

one class member is a citizen of a state different from the Defendant. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

13. This Court has personal jurisdiction over Defendant as Wawa maintains its principal executive offices in Wawa, Pennsylvania, is registered to conduct business in Pennsylvania, regularly conducts business in Pennsylvania, and has sufficient minimum contacts in Pennsylvania. Defendant intentionally avails itself of this jurisdiction by conducting its corporate operations here and promoting, selling, and marketing Wawa's services to resident Pennsylvania consumers and entities.

14. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to the claims of the Plaintiff occurred in this District.

FACTUAL ALLEGATIONS

A. Wawa's Data Breach

15. On December 19, 2019, Wawa announced a companywide Data Breach "at potentially all Wawa locations," which includes over 850 convenience retail stores and gas stations in seven states. Wawa discovered Malware on its payment processing servers that affected customer payment card information beginning at different points in time after March 4, 2019 until it was contained on December 12, 2019.

16. At different points in time after March 4, 2019, Malware began running on in-store payment processing systems at potentially all Wawa locations. The Malware was present on most store systems by approximately April 22, 2019.

17. The Malware affected Plaintiff's and Class Members' PII, by exposing their credit and debit card numbers, expiration dates, and names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers.

B. The Data Breach Caused Harm to Plaintiff and Class Members

18. PII such as affected credit and debit card numbers, expiration dates, and cardholder names is highly coveted data and a frequent target of hackers.

19. Despite well-publicized litigation and frequent public announcements of data breaches, especially in the retail sector, Wawa maintained an insufficient and inadequate system to protect Plaintiff's and Class Members' PII.

20. Payment card data such as credit or debit card information is highly valuable to hackers. Identity thieves use this stolen PII for a variety of financial fraud related crimes. Credit and debit card information that is stolen from the point of sale is known as "dumps." Credit and debit card dumps can then be sold in the cybercrime underground. This information can also be used to fraudulently clone a debit or credit card.

21. Wawa failed to implement and maintain reasonable security procedures and practices appropriate to protect Plaintiff's and Class Members' PII.

22. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, including PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS.³

23. Under the FTC guidelines, businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities;

³ FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Oct. 2016), *available at* <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

24. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

25. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 (2006). Wawa’s failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

26. Here, Wawa was at all times fully aware of its obligation to protect the personal and financial data of its customers because of its participation in the storage of PII, storage of payment card data, and interactions with payment card processing networks.

27. Wawa was also aware of the significant repercussions if it failed to do so because Wawa collected payment card data from tens of thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class Members.

28. Despite understanding the consequences of inadequate data security, Wawa failed to take appropriate protective measures to protect and secure customers' PII, including Plaintiff and Class Members.

29. Despite understanding the consequences of inadequate data security, Wawa failed to take other measures necessary to protect its data network.

30. In the case of a data breach, merely reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."⁴

31. A victim whose PII has been stolen and compromised may not see the full extent of identity theft or fraud until years after the initial breach. It may take some time for the victim to become aware of the theft. In addition, a victim may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

32. According to the BJS, an estimated 16.6 million people were victims of one or more incidents of identity theft in 2012. Among identity theft victims, existing bank or credit card accounts were the most common types of misused information.⁵

33. Without detailed disclosure to Wawa's customers, Plaintiff and Class Members were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their PII for months without being able to take necessary precautions to prevent

⁴ See Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft, 2012*, U.S. Department of Justice, Bureau of Justice Statistics (Dec. 2013), at 1.

⁵ *Id.*

imminent harm.

34. As a result of the Data Breach, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

35. Plaintiff and Class Members are also subject to a higher risk of phishing where hackers exploit information they already obtained to get even more PII. Plaintiff and Class Members are presently incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the bank or credit card companies

36. The exposure of Plaintiff's and Class Members' PII to Malware was a direct and proximate result of Wawa's failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure. Wawa failed to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII in order to protect such PII against reasonably foreseeable threats to the security of such information.

37. Plaintiff's and Class Members' PII is private and sensitive in nature and was inadequately protected by Wawa.

38. As one of the mid-Atlantic's leading convenience store and gas station chains with over 850 locations, Wawa had the sophisticated financial and technical resources to prevent such a Malware breach. However, Wawa has neglected to adequately invest in data security, despite the growing number of data intrusions and several years of well-publicized retail industry data breaches.

39. Had Wawa remedied the deficiencies in its information storage and security

systems, followed industry guidelines, and adopted measures recommended by the FTC and experts in the field, Wawa would have prevented intrusion into its payment storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

40. As a direct and proximate result of Wawa's wrongful actions and inaction, Plaintiff and Class Members have been placed at an immediate and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Wawa Data Breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

41. Wawa's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. The improper disclosure, compromising and theft of their PII;
- b. Unauthorized charges on their debit and credit card accounts;
- c. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized parties and misused via the sale of Plaintiff's and Class Members' PII on the internet black market and dark web;
- d. The untimely and inadequate notification of the Data Breach;
- e. Loss of privacy;
- f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
- g. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

- h. Loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and
- i. The loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

42. While Plaintiff's and Class Members' PII has been stolen, Wawa continues to hold Plaintiff's and Class Members' PII on their payment servers. Since Wawa has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

43. In response to the Data Breach, Wawa has "arranged with Experian to provide potentially impacted customers with one year of identity theft protection and credit monitoring at no charge."⁶ As previously alleged, Plaintiff's and Class Members' PII may exist on the dark web for months, or even years, before it is purchased and used by hackers. With only one year of monitoring, and no form of insurance or other protection, Plaintiff and Class Members remain unprotected from the real and long-term threats against their PII. Therefore, the "monitoring" services are inadequate, and Plaintiff and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

⁶ See <https://www.wawa.com/alerts/data-security>. However, credit reporting agencies such as Experian are themselves not immune to data breach intrusions. In September 2017, Equifax announced a data breach that exposed the personal information of 147 million people. See <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>.

CLASS ACTION ALLEGATIONS

44. Plaintiff, Nicholas Rapak, brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all others similarly situated, as representative of the following Class:

All persons residing in the United States who provided PII to Defendant and whose PII was accessed, compromised, or stolen as a result of the Data Breach disclosed by Defendant on December 19, 2019.

45. The aforementioned Class is referred to herein as the “Class.”

46. Excluded from the Class are affiliates, predecessors, successors, officers, directors, agents, servants, or employees of Defendant, and the immediate family members of such persons. Also excluded are any trial judge who may preside over this action and their law clerks, court personnel and their family members, and any juror assigned to this action.

47. Plaintiff reserves the right to amend the Class definition if discovery and/or further investigation reveal that it should be modified.

48. The members of the Class are so *numerous* that the joinder of all members of the Class in single action is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, Wawa has acknowledged that its customers’ PII was compromised for over nine months. Therefore, it stands to reason that the number of Class Members is likely in the millions. The Class Members are readily identifiable from information and records in Defendant’s possession, custody, or control, such as transaction records and purchases.

49. There are *common questions of law and fact* to the Class Members, which *predominate* over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant owed a duty to Plaintiff and Class Members to safeguard and

protect the security of their PII;

- b. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class Members' PII;
- c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class Members' PII from unauthorized capture, dissemination and misuse;

50. Plaintiff's claims are *typical* of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was misused, improperly disclosed by Defendant.

51. Plaintiff will fairly and *adequately represent* and protect the interests of the Class. Plaintiff has retained competent counsel experienced in litigation of complex class actions, including consumer class actions. Plaintiff intends to prosecute this action vigorously. Plaintiff's claims are typical of the claims of all of the other Class Members, and Plaintiff has the same non-conflicting interests as the other Class Members. Therefore, the interests of the Class Members will be fairly and adequately represented by Plaintiff and his counsel.

52. A class action is *superior* to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go un-remedied.

53. Class certification is appropriate under FED. R. CIV. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, such that

final injunctive or corresponding declaratory relief is appropriate to the Class as a whole.

CLAIMS FOR RELIEF

COUNT I
(Negligence)

54. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

55. Wawa owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

56. This duty included, among other things, designing, maintaining, and testing Wawa's security systems to ensure that Plaintiff's and Class Members' PII was adequately secured and protected. Wawa further had a duty to implement processes that would detect a breach of their security system in a timely manner.

57. Wawa also had a duty to timely disclose to Plaintiff and Class Members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff and Class Members could take appropriate measures to cancel or change their debit or credit cards, to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts, and take all other appropriate precautions.

58. Wawa breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information; allowing unauthorized access to Plaintiff's and Class Members' PII stored by Wawa, and failing to recognize in a timely manner the breach.

59. Wawa breached its duty to timely disclose that Plaintiff's and Class Members' PII had been, or was reasonably believed to have been, stolen or compromised.

60. Wawa's failure to comply with industry regulations and the delay between the date of intrusion and the date Wawa informed customers of the Data Breach further evidence Wawa's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

61. But for Wawa's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised, stolen, and viewed by unauthorized persons.

62. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Wawa's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII. Wawa knew or should have known that their systems and technologies for processing and securing Plaintiff's and Class Members' PII had security vulnerabilities susceptible to Malware.

63. As a result of Wawa's negligence, Plaintiff and Class Members incurred damages including, but not limited to, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Wawa's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit and debit cards of Wawa's customers by identity thieves who wrongfully gained access to the PII of

Plaintiff and Class Members.

COUNT II
(Negligence *Per Se*)

64. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

65. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by companies such as Wawa’s failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Wawa’s duty.

66. Wawa violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff’s and Class Members’ PII and not complying with industry standards. Wawa’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach at one of the mid-Atlantic’s largest convenience store and gas station chains.

67. Wawa’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

68. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

69. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

70. As a direct and proximate result of Wawa’s negligence, Plaintiff and Class

Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
(Breach of Implied Contract)

71. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

72. When Plaintiff and Class Members paid money and provided their PII to Wawa in exchange for goods and services, they entered into implied contracts with Wawa pursuant to which Wawa agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

73. Wawa solicited and invited prospective consumers such as Plaintiff and Class Members to provide their PII as part of its regular business practices by using their credit and/or debit cards. Plaintiff and Class Members accepted Wawa's offers and provided their PII to Wawa.

74. In entering into such implied contracts, Plaintiff and Class Members assumed that Wawa's data security practices and policies were reasonable and consistent with industry standards, and that Wawa would use part of the funds received from Plaintiff and Class Members to pay for adequate and reasonable data security practices.

75. Plaintiff and Class Members would not have entrusted their PII to Wawa in the absence of the implied contract between them and Wawa to keep the information secure.

76. Plaintiff and Class Members fully performed their obligations under the implied contracts with Wawa.

77. Wawa breached their implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice

that their PII was compromised as a result of the Data Breach.

78. As a direct and proximate result of Wawa's breaches of their implied contracts, Plaintiff and Class Members sustained actual losses and damages, including, but not limited to, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Wawa's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit and debit cards of Wawa's customers by identity thieves who wrongfully gained access to the PII of Plaintiff and Class Members.

COUNT IV

**(For Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law)
73 P.S. § 201-1 *et seq.*)**

79. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

80. As a consumer of Wawa's services, Plaintiff is authorized to bring a private action under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTCPL"). 73 P.S. § 201-9.2.

81. Plaintiff is a "person" within the meaning of 73 P.S. § 201-2(2).

82. Plaintiff and Class Members provided their PII to Wawa pursuant to transactions in "trade" and "commerce" as meant by 73 P.S. §201-2(3), for personal, family, and/or household purposes.

83. The UTCPL prohibits "unfair or deceptive acts or practices in the conduct of

any trade or commerce[.]” 73 P.S. § 201-3.

84. This Count is brought for Wawa’s unfair and deceptive conduct, including Wawa’s unlawful and unfair and deceptive acts and practices, which “creat[ed] a likelihood of confusion or of misunderstanding” for Plaintiff and Class Members as meant by 73 P.S. § 201-2(4)(xxi).

85. Wawa engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale and advertisement of the goods purchased by Plaintiff and the Class in violation of 73 P.S. § 201-3, including but not limited to the following:

- a. Wawa failed to enact adequate privacy and security measures to protect Plaintiff’s and Class Members’ PII from unauthorized disclosure, release, data breaches, Malware, and theft, which was a direct and proximate cause of the Data Breach;
- b. Wawa negligently represented that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff’s and Class Members’ PII from unauthorized disclosure, release, data breaches, Malware and theft was unfair and deceptive given the inadequacy of its privacy and security protections; and
- c. Wawa’s negligence in failing to disclose the material fact of the inadequacy of its privacy and security protections for Plaintiff and Class Members was unfair and deceptive.

86. The above unfair and deceptive acts and practices by Wawa were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

87. Wawa knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff’s Class Members’ PII and that risk of a data breach or theft was highly likely. Wawa’s actions in engaging in the above-named deceptive acts and practices were negligent, knowing and reckless with respect to the rights of members of the Class.

88. Plaintiff and Class Members relied on Wawa's unfair and deceptive acts and practices when they paid money in exchange for goods and services and provided their PII through Wawa's in-store payment terminals and fuel dispensers.

89. Plaintiff and Class Members relied on Wawa to safeguard and protect their PII and to timely and accurately notify them if their data had been breached and compromised.

90. Plaintiff and Class Members seek all available relief under the UTPCPL, 73 P.S. § 201-1 *et seq.*

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, Nicholas Rapak, individually and on behalf of the Class, respectfully requests that the Court:

- A. Certify the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class Members;
- B. Designate Plaintiff as representative of the Class and the undersigned counsel, LOWEY DANNENBERG, P.C. as Class Counsel;
- C. Award Plaintiff and the Class compensatory damages in an amount to be determined by the Court and treble and punitive damages to punish Defendant's egregious conduct as described herein, and to deter Defendant and others from engaging in similar conduct;
- D. Award Plaintiff and the Class injunctive relief, as permitted by law or equity, including enjoining Defendant from continuing the unlawful practices set forth herein, ordering Defendant to fully disclose the extent and nature of the security breach and theft, and ordering Defendant to pay for not less than three years of identity theft and credit card monitoring services for Plaintiff and the Class;
- E. Award Plaintiff and the Class statutory interest and penalties;
- F. Award Plaintiff and the Class their costs, prejudgment and post judgment interest, and attorneys' fees; and
- G. Grant such other relief that the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury as to all issues stated herein, and all issues so triable.

Dated: December 20, 2019
West Conshohocken, PA

Respectfully submitted,

By: 

Anthony M. Christina (PA ID# 322528)
LOWEY DANNENBERG, P.C
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Email: achristina@lowey.com

Vincent Briganti (*pro hac vice* forthcoming)
Christian Levis (*pro hac vice* forthcoming)
Johnathan Seredynski (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Email: vbriganti@lowey.com
clevis@lowey.com
jseredynski@lowey.com

Attorneys for Plaintiff Nicholas Rapak and the Proposed Class